II. REMARKS

A. Status of the Claims:

Claims 1-31 were pending prior to this preliminary amendment. Claims 7-11, 17-21, and 26-31 are presently pending. Claims 1-6, 12-16, and 22-25 have been cancelled. Claims 7-11, 18-19, 21, and 26-31 have been amended in this preliminary amendment. No new matter has been introduced. The attached appendices reflect the amendments and the pending claims for the convenience of the Office.

Claims 8-9, 11, 18-19, 21, 27-29, and 31 were amended for purely cosmetic reasons. No change in meaning or scope of the claims is intended or expected by reason of the amendments.

Claims 7, 10, 26, and 30 were amended to directly incorporate limitations already present in the claims by virtue of their ultimate dependencies. Therefore, no change in meaning or scope of the claims is intended or expected by reason of the amendments.

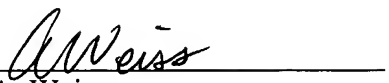
III. CONCLUSION

Applicant believes that the Examiner should swiftly pass the pending claims to issuance.

Should any additional fees be required under Rules 1.16 – 1.21 for any reason relating to the enclosed materials, the Assistant Commissioner is authorized to deduct said fees from Thompson & Knight, LLP's Deposit Account No. 20-0821/501143.000008/AAW.

Respectfully submitted,

Date: January 9, 2003



Aaron A. Weiss
Reg. No. 46,163

THOMPSON & KNIGHT LLP
1200 San Jacinto Center
98 San Jacinto Boulevard
Austin, TX 78701-4081
(512) 469-6100

ATTORNEYS FOR APPLICANT

APPENDIX A

SPECIFICATION AMENDMENTS

Page 4, line 23 - page 5, line 5:

A preferred embodiment is a data encryption method performed with ring arithmetic operations ~~using a residue number multiplication process wherein a first conversion to a first basis is done using a mixed radix system and a second conversion to a second basis is done using a mixed radix system. In some embodiments,~~ wherein a modulus C is to be chosen of the form $2^w - L$, wherein C is a w-bit number and L is a low Hamming weight odd integer less than $2^{(w-1)/2}$. And in some of those embodiments, the residue mod C is calculated via several steps. P is split into 2 w-bit words H_1 and L_1. S_1 is calculated as equal to $L_1 + (H_1 2^{x1}) + (H_1 2^{x2}) + \ldots + (H_1 2^{xk}) + H_1$. S_1 is split into two w-bit words H_2 and L_2. S_2 is computed as being equal to $L_2 + (H_2 2^{x1}) + (H_2 2^{x2}) + \ldots + (H_2 2^{xk}) + H_2$. S_3 is computed as being equal to $S_2 + (2^{x1} + \ldots + 2^{xk} + 1)$. And the residue is determined by comparing S_3 to 2^w. If $S_3 < 2^w$, then the residue equals S_2. If $S_3 \geq 2^w$, then the residue equals $S_3 - 2^w$.

Page 17, lines 2-7:

The shotgun multiplication method, as well as other methods, can be used more efficiently by choosing the bases ($m_1, \ldots m_{2t}$) in ways that make the modular calculations simpler. A w-bit number C is a "castout modulus" if it is of the form $2^w - L$, where L is a low Hamming weight odd integer less than $2^{(w-3)/2}$, i.e., $C = 2^w - 2^{x1} - 2^{x2} - \ldots - 2^{xk} - 1$, where $(w - 3)/2 > x_1 > x_2 > \ldots > x_k > 0$ and k is much less than w. The "castout order" of C is defined to be one less than the Hamming weight of L.

Abstract, Page 37, lines 3-13:

A data encryption method performed with ring arithmetic operations ~~using a residue number multiplication process wherein a first conversion to a first basis is done using a mixed radix system and a second conversion to a second basis is done using a mixed radix system. In some embodiments,~~ wherein a modulus C is to be chosen of the form $2^w - L$, wherein C is a w-bit number and L is a low Hamming weight odd integer less than $2^{(w-1)/2}$. And in some of those embodiments, the residue mod C is calculated via several steps. P is split into 2 w-bit words H_1 and L_1. S_1 is calculated as equal to $L_1 + (H_1 2^{x1}) + (H_1 2^{x2}) + \ldots + (H_1 2^{xk}) + H_1$. S_1 is split into two w-bit words H_2 and L_2. S_2 is computed as being equal to $L_2 + (H_2 2^{x1}) + (H_2 2^{x2}) + \ldots + (H_2 2^{xk}) + H_2$. S_3 is computed as being equal to $S_2 + (2^{x1} + \ldots + 2^{xk} + 1)$. And the residue is determined by comparing S_3 to 2^w. If $S_3 < 2^w$, then the residue equals S_2. If $S_3 \geq 2^w$, then the residue equals $S_3 - 2^w$.

CLAIM AMENDMENTS

7. (Amended) [The method of claim A1, further] A method of encrypting data comprising:

performing a ring arithmetic function on numbers, including:

using a residue number multiplication process;

converting to a first basis using a mixed radix system;

converting to a second basis using a mixed radix system;

choosing a modulus C for modular calculations;

wherein the modulus C is w-big; and

wherein the modulus C is w-heavy.

8. (Amended) The method of claim [A7] 7,

wherein the modulus C is of the form $2^w - L$; and

wherein L is a low Hamming weight odd integer less than $2^{(w-1)/2}$.

9. (Amended) The method of claim [A8] 8, further comprising:

calculating the modulus C by a process including:

splitting P into 2 w-bit words H_1 and L_1;

calculating $S_1 = L_1 + (H_1 2^{x1}) + (H_1 2^{x2}) + \ldots + (H_1 2^{xk}) + H_1$;

splitting S_1 into two w-bit words H_2 and L_2;

computing $S_2 = L_2 + (H_2 2^{x1}) + (H_2 2^{x2}) + \ldots + (H_2 2^{xk}) + H_2$;

computing $S_3 = S_2 + (2^{x1} + \ldots + 2^{xk} + 1)$;

determining the modulus C by comparing S_3 to 2^w, wherein the modulus $C = S_2$ if $S_3 < 2^w$, and wherein the modulus $C = S_3 - 2^w$ if $S_3 \geq 2^w$; and

wherein the modulus C is a residue.

10. (Amended) [The method of claim A1, further] A method of encrypting data comprising:

performing a ring arithmetic function on numbers, including:

using a residue number multiplication process;

converting to a first basis using a mixed radix system;

converting to a second basis using a mixed radix system;

choosing a modulus C for modular calculations;

wherein the modulus C is w-little; and

wherein the modulus C is w-light.

11. (Amended) The method of claim [A10] 10,

wherein the modulus C is of the form $2^w + L$; and

wherein the modulus C has a Hamming weight close to 1.

17. A method of encrypting data comprising:

choosing a modulus C for modular calculations;

wherein the modulus C is w-big; and

wherein the modulus C is w-heavy.

18. (Amended) The method of claim [C1] 17,

wherein the modulus C is of the form $2^w - L$; and

wherein L is a low Hamming weight odd integer less than $2^{(w-1)/2}$.

19. (Amended) The method of claim [C2] 18, further comprising:

calculating the modulus C by a process including:

splitting P into 2 w-bit words H_1 and L_1;

calculating $S_1 = L_1 + (H_1 2^{x1}) + (H_1 2^{x2}) + \ldots + (H_1 2^{xk}) + H_1$;

splitting S_1 into two w-bit words H_2 and L_2;

computing $S_2 = L_2 + (H_2 2^{x1}) + (H_2 2^{x2}) + \ldots + (H_2 2^{xk}) + H_2$;

computing $S_3 = S_2 + (2^{x1} + \ldots + 2^{xk} + 1)$;

determining the modulus C by comparing S_3 to 2^w, wherein the modulus $C = S_2$ if $S_3 < 2^w$, and wherein the modulus $C = S_3 - 2^w$ if $S_3 \geq 2^w$; and

wherein the modulus C is a residue.

20. A method of encrypting data comprising:

choosing a modulus C for modular calculations;

wherein the modulus C is w-little; and

wherein the modulus C is w-light.

21. (Amended) The method of claim [D1] 20,

wherein the modulus C is of the form $2^w + L$; and

wherein the modulus C has a Hamming weight close to 1.

26. (Amended) [The method of claim E1, further] A method of hashing data comprising:

performing a ring arithmetic function on numbers, including:

using a residue number multiplication process;

converting to a first basis using a mixed radix system;

converting to a second basis using a mixed radix system;

choosing a modulus C for modular calculations;

wherein the modulus C is w-big; and

wherein the modulus C is w-heavy.

27. (Amended) The method of claim [E5] 26,

wherein the modulus C is of the form $2^w - L$; and

wherein L is a low Hamming weight odd integer less than $2^{(w-1)/2}$.

28. (Amended) The method of claim [E6] 27, further comprising

calculating the modulus C by a process including:

splitting P into 2 w-bit words H_1 and L_1;

calculating $S_1 = L_1 + (H_1 2^{x1}) + (H_1 2^{x2}) + \ldots + (H_1 2^{xk}) + H_1$;

splitting S_1 into two w-bit words H_2 and L_2;

computing $S_2 = L_2 + (H_2 2^{x1}) + (H_2 2^{x2}) + \ldots + (H_2 2^{xk}) + H_2$;

computing $S_3 = S_2 + (2^{x1} + \ldots + 2^{xk} + 1)$;

determining the modulus C by comparing S_3 to 2^w, wherein the modulus $C = S_2$ if $S_3 < 2^w$, and wherein the modulus $C = S_3 - 2^w$ if $S_3 \geq 2^w$; and

wherein the modulus C is a residue.

29. (Amended) The method of Claim [E7] 28, wherein the method of hashing data comprises a method of cryptographic hashing.

30. (Amended) [The method of claim E1, further] A method of hashing data comprising:

performing a ring arithmetic function on numbers, including:

using a residue number multiplication process;

converting to a first basis using a mixed radix system;

converting to a second basis using a mixed radix system;

choosing a modulus C for modular calculations;

wherein the modulus C is w-little; and

wherein the modulus C is w-light.

31. (Amended) The method of claim [E9] 30,

wherein the modulus C is of the form $2^w + L$; and

wherein the modulus C has a Hamming weight close to 1.

APPENDIX B

PENDING CLAIMS

7. (Amended) A method of encrypting data comprising:

performing a ring arithmetic function on numbers, including:

using a residue number multiplication process;

converting to a first basis using a mixed radix system;

converting to a second basis using a mixed radix system;

choosing a modulus C for modular calculations;

wherein the modulus C is w-big; and

wherein the modulus C is w-heavy.

8. (Amended) The method of claim 7,

wherein the modulus C is of the form $2^w - L$; and

wherein L is a low Hamming weight odd integer less than $2^{(w-1)/2}$.

9. (Amended) The method of claim 8, further comprising:

calculating the modulus C by a process including:

splitting P into 2 w-bit words H_1 and L_1;

calculating $S_1 = L_1 + (H_1 2^{x1}) + (H_1 2^{x2}) + \ldots + (H_1 2^{xk}) + H_1$;

splitting S_1 into two w-bit words H_2 and L_2;

computing $S_2 = L_2 + (H_2 2^{x1}) + (H_2 2^{x2}) + \ldots + (H_2 2^{xk}) + H_2$;

computing $S_3 = S_2 + (2^{xl} + \ldots + 2^{xk} + 1)$;

determining the modulus C by comparing S_3 to 2^w, wherein the modulus $C = S_2$ if $S_3 < 2^w$, and wherein the modulus $C = S_3 - 2^w$ if $S_3 \geq 2^w$; and

wherein the modulus C is a residue.

10. (Amended) A method of encrypting data comprising:

performing a ring arithmetic function on numbers, including:

using a residue number multiplication process;

converting to a first basis using a mixed radix system;

converting to a second basis using a mixed radix system;

choosing a modulus C for modular calculations;

wherein the modulus C is w-little; and

wherein the modulus C is w-light.

11. (Amended) The method of claim 10,

wherein the modulus C is of the form $2^w + L$; and

wherein the modulus C has a Hamming weight close to 1.

17. A method of encrypting data comprising:

choosing a modulus C for modular calculations;

wherein the modulus C is w-big; and

wherein the modulus C is w-heavy.

18. (Amended) The method of claim 17,

wherein the modulus C is of the form $2^w - L$; and

wherein L is a low Hamming weight odd integer less than $2^{(w-1)/2}$.

19. (Amended) The method of claim 18, further comprising:

calculating the modulus C by a process including:

splitting P into 2 w-bit words H_1 and L_1;

calculating $S_1 = L_1 + (H_1 2^{x1}) + (H_1 2^{x2}) + \ldots + (H_1 2^{xk}) + H_1$;

splitting S_1 into two w-bit words H_2 and L_2;

computing $S_2 = L_2 + (H_2 2^{x1}) + (H_2 2^{x2}) + \ldots + (H_2 2^{xk}) + H_2$;

computing $S_3 = S_2 + (2^{x1} + \ldots + 2^{xk} + 1)$;

determining the modulus C by comparing S_3 to 2^w, wherein the modulus $C = S_2$ if $S_3 < 2^w$, and wherein the modulus $C = S_3 - 2^w$ if $S_3 \geq 2^w$; and

wherein the modulus C is a residue.

20. A method of encrypting data comprising:

choosing a modulus C for modular calculations;

wherein the modulus C is w-little; and

wherein the modulus C is w-light.

21. (Amended) The method of claim 20,

wherein the modulus C is of the form $2^w + L$; and

wherein the modulus C has a Hamming weight close to 1.

26. (Amended) A method of hashing data comprising:

performing a ring arithmetic function on numbers, including:

using a residue number multiplication process;

converting to a first basis using a mixed radix system;

converting to a second basis using a mixed radix system;

choosing a modulus C for modular calculations;

wherein the modulus C is w-big; and

wherein the modulus C is w-heavy.

27. (Amended) The method of claim 26,

wherein the modulus C is of the form $2^w - L$; and

wherein L is a low Hamming weight odd integer less than $2^{(w-1)/2}$.

28. (Amended) The method of claim 27, further comprising

calculating the modulus C by a process including:

splitting P into 2 w-bit words H_1 and L_1;

calculating $S_1 = L_1 + (H_1 2^{x1}) + (H_1 2^{x2}) + \ldots + (H_1 2^{xk}) + H_1$;

splitting S_1 into two w-bit words H_2 and L_2;

computing $S_2 = L_2 + (H_2 2^{x1}) + (H_2 2^{x2}) + \ldots + (H_2 2^{xk}) + H_2$;

computing $S_3 = S_2 + (2^{x1} + \ldots + 2^{xk} + 1)$;

determining the modulus C by comparing S_3 to 2^w, wherein the modulus $C = S_2$ if $S_3 < 2^w$, and wherein the modulus $C = S_3 - 2^w$ if $S_3 \geq 2^w$; and

wherein the modulus C is a residue.

29. (Amended) The method of Claim 28, wherein the method of hashing data comprises a method of cryptographic hashing.

30. (Amended) A method of hashing data comprising:

performing a ring arithmetic function on numbers, including:

using a residue number multiplication process;

converting to a first basis using a mixed radix system;

converting to a second basis using a mixed radix system;

choosing a modulus C for modular calculations;

wherein the modulus C is w-little; and

wherein the modulus C is w-light.

31. (Amended) The method of claim 30,

wherein the modulus C is of the form $2^w + L$; and

wherein the modulus C has a Hamming weight close to 1.